

**Diane Reynolds, on behalf of herself and
all others similarly situated,**

15111 Glade Drive
Apt. 2G
Silver Spring, MD 20906

Plaintiff,

v.

Athena Bitcoin, Inc.

1332 North Halsted Street
Suite 401
Chicago, IL 60642

Serve on:

Incorp. Services, Inc.
1519 York Road
Lutherville, MD 21093

and

Genesis Coin, Inc.

c/o Andrew Barnard, CEO
1541 Sunset Drive
Suite 202
Coral Gables, FL 33143

Defendants.

* * * * *

**CLASS ACTION COMPLAINT
AND DEMAND FOR JURY TRIAL**

Plaintiff Diane Reynolds (“Named Plaintiff” or “Plaintiff”), on behalf of herself and all others similarly situated (the “Class”), files this Class Action Complaint and Demand for Jury Trial by and through undersigned counsel against Defendants Athena Bitcoin, Inc. (“Athena”) and Genesis Coin, Inc. (“Genesis”) (together, “Defendants”) and for cause states:

BACKGROUND

1. Elder financial scams are both rampant and increasing in the United States and in Maryland.

2. The Federal Trade Commission (“FTC” or the “Commission”) reported that in 2023 alone, elder financial scams accounted for a reported loss of \$1.9 billion, an increase from the reported \$1.6 billion lost in 2022. Because most fraud isn’t reported, the actual figure could be as high as \$61.5 billion. The FTC also found that older adults have higher median losses than younger adults.

3. Many elder financial scams involve cryptocurrency transactions, which are untraceable, do not have legal protections, and are not reversible.

4. The Commission reported that older adults are especially vulnerable to scams involving payments made using cryptocurrency, such as Bitcoin.

5. While the largest share of cryptocurrency losses reported by older adults stem from investment scams, nearly half of reports involved business impersonation, tech support scams, and government impersonation scams. The number of reports about cryptocurrency payments by older adults on business impersonation, government impersonation, and tech support scams increased by over 80%, from 2,304 in 2022 to 4,191 in 2023.

6. The FTC noted that victims of those scams “often report being directed to [Bitcoin Automatic Teller Machine (“ATMs”)] to deposit cash.”¹

7. Bitcoin ATMs are free-standing kiosks akin to traditional Automated Teller Machines.

8. Bitcoin ATMs permit customers to buy or sell cryptocurrency assets (including Bitcoin) in exchange for cash issued by sovereign governments liked the United States.

¹ FTC Consumer Protection Data Spotlight, *Bitcoin ATMs: A payment portal for scammers* (Sept. 3, 2024), available at <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers>.

9. The Commission found a nearly tenfold increase since 2020 in the amount lost to scammers using Bitcoin ATMs—from \$12 million to \$114 million. In the first half of 2024 alone, victims lost a staggering \$65 million in Bitcoin ATM-related scams.

10. Bitcoin-ATM related fraud is so prevalent that even those bullish on cryptocurrency and its decentralized nature have found Bitcoin ATMs to be problematic.²

11. In these types of scams, the scammer places the victim under duress by threatening dangers that require urgent action to protect the victim’s physical or financial well-being. Then, the scammer convinces the victim that the only way to avert the threatened danger is to deposit cash into a cryptocurrency-vending ATM, which converts U.S. Dollars into an untraceable cryptocurrency and transfers the Bitcoin to a “secure” Bitcoin wallet. The scammer then sends the user a QR code and instructs the user to hold the QR code up to the ATM camera. The QR code is embedded with the scammer’s Bitcoin wallet address, causing the deposit of the Bitcoin directly into the scammer’s online Bitcoin wallet.

12. Defendants have long known that Athena ATMs are exploited by criminals to facilitate illegal activity such as fraud, money laundering, and scams, including cryptocurrency ATM scams.

13. In fact, on September 12, 2024, United States Senator Dick Durbin of Illinois led a group of seven Senators in pressing the ten largest Bitcoin ATM operators, including Athena, to curb such fraud against elderly Americans.

² Kevin Williams, *The bitcoin ATM has emerged as one of cryptocurrency’s biggest threats*, CNBC (Sept. 8, 2024), <https://www.cnbc.com/2024/09/08/biggest-risks-of-accessing-crypto-through-bitcoin-atm.html> (“Bitcoin is decentralized, permission-less, and immutable. ‘A transaction cannot be reversed or recalled if funds are deposited to the wrong address,’ And while many crypto bulls find bitcoin’s lack of governance appealing, that can be problematic in ATMs.”).

14. Despite their knowledge, Defendants have—for years—failed to prevent, intercept, and/or mitigate the elder financial scams involving Athena ATMs.

15. Defendants’ failures breached the duties they assumed to prevent, intercept, and mitigate elder financial abuse through Athena ATMs. To be sure, Defendants recognized the prevalence and severity of elder financial scams involving Athena ATMs and held themselves out to the public and their customers that it “ensures safe and secure banking”

16. Defendants also neglected to intervene in (*i.e.*, stop) such scams from happening. As such, Athena ATMs continued to be used in cryptocurrency scams, money laundering, and other illegal transactions.

17. Defendants, of course, have always been capable of implementing effective and sufficient checks and procedures both at the ATMs and internally that would have prevented, mitigated, or deterred the use of the ATMs in scams such as the one in this case. Defendants, however, knowingly chose to not adopt effective checks or balances because doing so would thwart a substantial volume of their business and the profits gained from every dollar inserted into the ATM.

18. Upon information and belief, the primary use of Athena ATMs is transactions related to fraud perpetrated against elders.³

³ See, e.g., Rob Wile & Christina Romans, *Bitcoin ATM scams are soaring – and older adults are increasingly the victims*, CNBC (Sept. 1, 2024), <https://www.cnbc.com/2024/09/01/bitcoin-atm-scams-surge-disproportionately-duping-older-adults.html> (“[R]oughly \$2 out of every \$3 lost in a scam involving a bitcoin ATM belonged to someone near or over retirement age.”); Williams, *supra* (“Although the bitcoin ATM isn’t exactly drawing crowds, Patel says a surprising number of senior citizens show up at the kiosk, alarming given the rise of bitcoin ATM scams targeting seniors.”).

19. In fact, traditional cryptocurrency trading platforms advise investors against using Bitcoin ATMs because they have higher transaction fees compared to other transaction methods.⁴ Put differently, a typical cryptocurrency investor has little incentive to use a Bitcoin ATM.

20. In their SEC filings, Athena acknowledges that their “total revenue is substantially dependent on the volume of transactions conducted by our customers. If such volume declines, our business, operating results, and financial position would be adversely affected.”

21. Defendants’ incentive to turn a blind eye to fraud is devastating to older adult victims.

22. Plaintiff, for example, lost thousands of dollars due to Defendants’ negligent, reckless, and knowing failure and refusal to implement appropriate and sufficient measures and procedures to prevent, intervene, mitigate, and/or deter the use of ATMs in fraudulent activity.

23. Rather than pursue fixes that would effectively thwart escalating and rampant ATM-involved schemes, Defendants remain laser-focused on profits and their bottom lines.

24. Athena charges transaction fees between 20 and 25%. They are able to charge such high fees because scammers either don’t mind or are willing to pay higher fees due to the anonymity the service provides. And the victims don’t realize what’s happening.

25. Plaintiff and similarly situated class members are entitled to restitution, damages, penalties, injunctive relief, and other relief as appropriate.

PARTIES

26. Plaintiff Diane Reynolds is a resident of Montgomery County, Maryland. She is a resident of Silver Spring and has been at all times relevant to this action.

⁴ See, e.g., Coinbase, *Bitcoin ATMs: how to use them and how do they work?*, <https://www.coinbase.com/learn/tips-and-tutorials/bitcoin-atms-how-to-use-them-and-how-do-they-work> (last visited Jan. 14, 2025).

27. Defendant Athena Bitcoin, Inc. is a Delaware corporation headquartered in Illinois. Athena is not currently registered to do business in the State of Maryland; its license was forfeited in November 2024 for failure to file documents. Athena is a wholly-owned subsidiary of parent company Athena Bitcoin Global, a Nevada corporation founded in 1991 under the name “GamePlan, Inc.”

28. Defendant Genesis Coin, Inc. is a Delaware corporation that is headquartered in Florida. Genesis has never been licensed to do business in the State of Maryland.

JURISDICTION AND VENUE

29. This Court may properly exercise jurisdiction over Defendants pursuant to Md. Code, Cts. & Jud. Proc. § 6-103. Defendants transact or transacted business in Maryland. At all times relevant to this Complaint, Defendants purposefully placed, operated, maintained, and derived substantial revenue from approximately 138 separate Athena ATMs in Maryland, including the Athena Bitcoin ATM at issue in this case.

30. Venue in this District is proper pursuant to Md. Code, Cts. & Jud. Proc. §§ 6-201 and 6-202. Defendants carry on or carried on regular business within Montgomery County and the cause of action arose in Montgomery County.

FACTUAL ALLEGATIONS

A. Athena’s Bitcoin ATMs Facilitated Fraud

31. Athena was founded on September 18, 2015.

32. Athena’s parent company, Athena Bitcoin Global, was founded in 1991.

33. As of December 2024, Athena operates more than 3,000 ATMs across the United States, El Salvador, Colombia, Argentina, and Mexico.

34. Athena's ATMs allow customers to exchange their physical currency for cryptocurrency or other digital assets. Customers can deposit cash into the machines and receive cash from the machines.

35. Athena's ATMs are located in various strategic locations—especially service stations and convenience stores—and present themselves as traditional ATMs.

36. In its most recent SEC filing, Athena stated that its “site selection criteria and metrics are a closely guarded proprietary aspect of our business. In placing our ATMs, we employ a data driven strategy based on a multitude of factors.”

37. Upon information and belief, Defendants intentionally placed ATMs in neighborhoods with large shares of low-income families and older adults.

38. Upon information and belief, Defendants placed ATMs in those locations because Defendants desired a high volume of ATM transactions, even if caused by scams at the expense of elderly and/or desperate customers.

39. At all times relevant, Defendants paid stores a fixed monthly payment to host their ATMs.


40. Athena purchased its ATMs from Genesis.

41. Athena's ATMs are connected to the Internet and use either its own software or software from Genesis.

42. The software allows customers to log-in to their Bitcoin wallets, deposit cash, and convert cash to Bitcoin stored in their wallets.


43. The software allows Athena to monitor its ATM network and collect data. The software also allows Athena to disable an ATM if there is a security concern.


44. To use an Athena ATM, customers first select a range of Bitcoin to purchase. According to its SEC filings, the ATM “may ask you to provide a form of ID such as a state ID or a Driver’s License.”



ATHENA
BITCOIN

BUY OR SELL BITCOIN & MORE





How to buy Bitcoin for the first time on an ATHENA ATM

Step One: Get a Wallet App On Your Smart Phone

WHAT IS A BITCOIN WALLET?

A Bitcoin wallet is simply a place where you can use and store your bitcoin. It can be an app on a smartphone or PC, or it can be a dedicated hardware computer like the Trezor or Ledger. Bitcoin wallets store a collection of private keys that allow you to spend and transfer bitcoin across the world to other Bitcoin addresses. Most Bitcoin wallets will ask you to write down recovery details in case something happens to your phone. *It's important to keep your username and password or 12+ word recovery phrase private and written down on paper stored in a safe place. Unfortunately, we have seen cases of customers losing their bitcoin because they couldn't remember their recovery details.*

Step Two: Bring your Smart Phone To One of Our Machines

Touch the screen to begin and select “Buy coins” on the menu of the ATM. Select the range for the amount of cash you plan to insert from one of two options. The machine will then ask for your cell phone number. Input your ten-digit phone number using the keypad. The system will then text you a six-digit code that you will type in using the keypad.

The ATM may ask you to provide a form of ID such as a state ID or a Driver’s License. Follow the onscreen instructions to scan your ID. If you are not asked to provide an ID, continue with your transaction.



Graphic used on Athena’s 2024 SEC filing

45. Customers then select what type of cryptocurrency they wish to purchase in exchange for United States currency. The machine can then scan a QR code from the customer's (or, as is often the case, the fraud victim's) phone. The customer then inserts cash into the machine, bill by bill. According to its most recent SEC filing, "Athena Bitcoin transactions are broadcast within 15 minutes from the time you finish at the ATM."



Step Three: Choose Currency and Delivery Method

After entering your code, you will be asked which digital currency you would like to purchase. We currently offer **Bitcoin**, **Litecoin**, **Ether/ETH** and **Bitcoin Cash (BCH)**. Make sure you have a wallet or address compatible with the coin type you have chosen.

Next, the ATM will ask you where you want your digital currency to be sent. If you already have a mobile wallet, such as the Edge wallet, select "Scan Wallet QR Code" at the ATM. Also press the "Request" or "Receive" button in your mobile wallet to bring up your current address. Once your public address is displayed as a QR code (see image to the left), you may hold your phone's screen in front of the scanner's red light near the keypad. When the ATM recognizes your address it will show it on its screen as a long string of characters. You may compare the first and last digits of that address with the one on your phone to verify the address is correct. An example Bitcoin address is shown to the left under "Waiting for Payment..."

If you wish to input your address manually, select "Enter Address" at the ATM instead. If you do not currently have a mobile wallet or have trouble scanning a QR code, you can generate a new paper wallet by tapping "Create New Wallet" and then later transfer the funds to your mobile or PC wallet. See instructions at the end of this page for how to use a paper wallet.

Step Four: Insert Money, Receive Digital Currency

The machine will now prompt you to insert cash. Start inserting your bills one by one. Athena ATMs do not accept debit or credit cards, so bring cash. When you are done touch the "Finish" button on the screen and a receipt will print showing you exactly how much you have bought and the address it was sent to.

Usually posted to your wallet within 15 minutes

Athena Bitcoin transactions are broadcast within 15 minutes from the time you finish at the ATM. Please wait at least that long to see your transaction appear in your wallet. There are rare occasions where this may take longer. Refreshing or rescanning your wallet may be needed. Websites, especially, may not recognize a payment until the transaction confirms (10-30 minutes later, usually) even though they have technically received the bitcoin. You can verify if your transaction has been sent by checking your address on a block explorer.



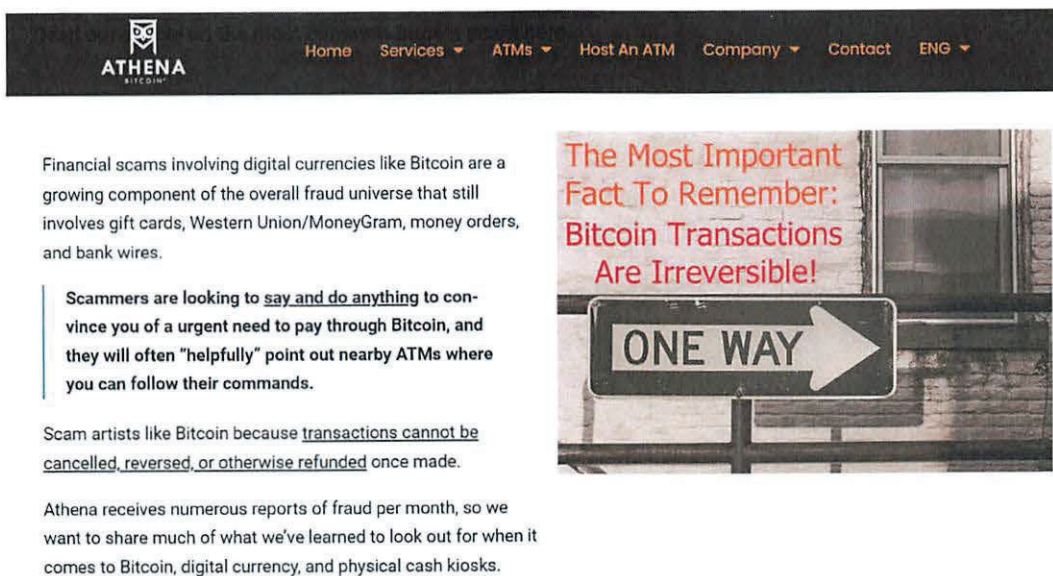
Graphic used on Athena's 2024 SEC filing

46. Defendants are engaged in the business of placing and operating cryptocurrency ATMs through which they sell shares of Bitcoin.

47. At all times relevant, Defendants knew that Athena ATMs were being exploited by criminals to facilitate illegal activity, such as fraud, money laundering, gambling, tax evasion, and scams.

48. In its latest SEC filing, Athena stated that one risk factor for its business operations and financial position is “existing and potential users may lose confidence in cryptocurrency-related products and services” and that one reason for the public’s lack of confidence is the number of related businesses being “sued, investigated, or shut down to do fraud, manipulative practices, business failure and security breaches.” They acknowledged that “[i]n many of these instances, customers of these businesses were not compensated or made whole for their losses.”

49. On its website, Athena published a section titled “Avoid these Bitcoin Scams.” On the website page, Athena recognized that “[s]cammers are looking to say and do anything to convince you of an urgent need to pay through Bitcoin, and they will often ‘helpfully’ point out nearby ATMs where you can follow their commands.”



50. On the same page of its website, Athena stated that it “receives numerous reports of fraud per month, so we want to share much of what we’ve learned to look out for when it comes to Bitcoin, digital currency, and physical cash kiosks.”

51. Further illustrating this point, Athena has received several complaints directly from consumers that they or a loved one had been victimized by scams utilizing Athena ATMs.

52. The Consumer Financial Protection Bureau’s records show complaints relating to Athena ATMs as early as January 2020.

53. Since around that time, news outlets have extensively covered the rise of crypto scams using Bitcoin ATMs to prey on vulnerable victims.

54. Yet Defendants have not taken steps that would curb these abuses. Moreover, Defendants are aware that the measures they have implemented are ineffective at curbing the escalating fraud occurring at its ATMs.

55. In its latest SEC filings, Defendants point to only a few security measures, all of which are obviously inadequate. For example, Defendants sometimes require customers/victims to insert a phone number, a driver’s license, or their Social Security Number. These measures do nothing to stop the most common form of Bitcoin ATM fraud, as scammers can easily direct their victims to input the requisite information.

56. Upon information and belief, Defendants do not use common-sense measures that have been suggested by experts in the field. For example, Defendants do not use transaction limits. Defendants do not hold transactions for a reasonable period when a first-time customer makes a large transfer—two states have passed legislation requiring as much. Defendants do not use analytics to screen for fraudulent transactions. And Defendants do not provide transaction receipts with transaction hashes that make it easier for law enforcement to trace and recover stolen funds.

These types of measures are likely to be effective at stemming fraud, but they would also likely cut into Defendants' bottom line.

57. Finally, Defendants do nothing to protect consumers from scams, such as inquiring about the basis for their transactions or reporting suspicious activity to appropriate authorities. Similar transactions would undoubtedly be scrutinized by personnel of a financial institution.

58. Defendants are capable of implementing effective procedures to prevent, deter, and mitigate these scams, but knowingly choose not to adopt them because doing so would reduce the immense profits they gain from every dollar inserted into an ATM.

B. Plaintiff's Story

59. Plaintiff Diane Reynolds is a seventy-five-year-old woman who lives alone in Leisure World, a senior community located in Silver Spring, Maryland.

60. Plaintiff was the full-time caregiver for her mother until her mother passed away on December 1, 2024.

61. Plaintiff was the victim of a Bitcoin ATM scam.

62. On or about July 29, 2024, Plaintiff saw an alert on her laptop warning her of a security breach. After trying to regain control of the computer for approximately an hour, she called the number displayed on the screen, believing it to be associated with Apple. The person who answered the phone told Plaintiff that several hackers involved with pornography were accessing her computer. He asked Plaintiff where she banked, and when she said Wells Fargo, the person on the phone claimed to transfer the call to Wells Fargo Bank.

63. The fake Wells Fargo representative called himself Michael Davis. The scammer claimed to be in touch with the Department of Justice. He told Plaintiff that the hackers planned to remove lots of money from her account and that she needed to withdraw it before they could do

so. He instructed Plaintiff to take the cash to an Athena ATM “to be sure it would be encrypted.”

64. Plaintiff drove to Wells Fargo and, at the scammer’s urging, persuaded the teller to effectuate the withdrawal of \$13,000.

65. The scammer gave Plaintiff the address of an Athena ATM, located inside a Shell Gas Station at 4101 Randolph Road, Silver Spring, MD 20906. The location—which isn’t far from other Athena ATMs—is in a working-class neighborhood with a heavy immigrant population. It is close to Leisure World and several other senior communities. The area is not replete with crypto investors—or consumers who fit the but instead with potential fraud victims.

66. Plaintiff located the machine, and the scammer stayed on the phone with her through the transaction.

67. The scammer sent Plaintiff a QR code that she held up to the camera of the Athena ATM. She did not realize that the QR code was connected to the scammer’s Bitcoin wallet. She inserted each bill one after another into the machine. At the end of the transaction, the Athena ATM printed a receipt.

Athena Bitcoin
Kiosk #21888
4101 Randolph Rd
Silver Spring, MD 20906

Transaction ID: 4D5Q7RZ4
Currency: \$13100.00
Bitcoin: BTC 0.14538544
Address: 14k7fbb9UwHAPvAxpJUtzeVZN17K9B
G8a
Rate: \$90105.31
Date & time: 29 Jul '24, 04:37 PM

Phone support:
(312) 880-4466
Email support:
support@athenabitcoin.com
Website:
athenabitcoin.com

68. After the transfer, the scammer repeatedly called and texted Plaintiff, attempting to convince her to withdraw more money. This alarmed Plaintiff.

69. The next day, on or around July 30, 2024, Plaintiff received a fraud alert from Wells Fargo, which prompted her to go to the Montgomery County Police Department and file a report.

CLASS ACTION ALLEGATIONS

70. Plaintiff re-alleges and incorporates by reference herein all the allegations contained above.

71. Pursuant to Maryland Rule 2-231, Plaintiff asserts claims on behalf of the following **Class: All Marylanders 68 and older, currently living or deceased, who were victims of a financial scam involving an Athena ATM from February 6, 2020 to the present.**

72. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; all judges assigned to hear any aspect of this litigation, as well as their immediate family members; and any individuals who have been granted a discharge pursuant to the United States Bankruptcy Code or state receivership laws after the date of the fraudulent transaction using one of Defendants' machines.

73. The Class, as defined above, is identifiable. Named Plaintiff is a member of the class.

74. Upon information and belief, the Class consists, at a minimum, of several dozen Maryland seniors and is thus so numerous that joinder of all members is clearly impracticable.

75. There are questions of law and fact which are not only common to the Class but which predominate over any questions affecting individual class members.

76. The common and predominating questions for the Class include, but are not limited to:

- a. Whether Defendants knew or should have known of the susceptibility of Plaintiff and Class Members in financial scams involving Athena ATMs;
- b. Whether Defendants financially exploited Plaintiff and Class Members by facilitating fraud on Athena ATMs;
- c. Whether Defendants' security procedures and practices to intervene, prevent, mitigate, and/or deter financial scams involving its Athena ATMs were reasonable;
- d. Whether Defendants have knowledge that its Athena ATMs are used by criminals to engage in transactions for illegal goods and services, including drug sales and trafficking, human trafficking, and prostitution;
- e. Whether Defendants failed to design and manufacture its Athena ATMs to deter the victimization of its users;
- f. Whether Plaintiff and Class Members are entitled to actual and/or treble damages and/or whether injunctive, corrective, and/or declaratory relief is/are appropriate as a result of Defendants' wrongful conduct; and
- g. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

77. Plaintiff's claims are typical of the claims of the Class Members within the meaning of Maryland Rule 2-231(b)(3) and are based on and arise out of similar facts constituting the wrongful conduct of Defendants. The prosecution of separate actions by individual members of the Class would create a risk of establishing incompatible standards of conduct for Defendants, within the meaning of Maryland Rule 2-231(c)(1)(A).

78. Common questions of law and fact enumerated above predominate over questions affecting only individual members of the Class, and a class action is the superior method for fair and efficient adjudication of the controversy, within the meaning of Rule 2-231(c)(3). The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to conduct such litigation.

79. Plaintiffs' counsel is experienced in class actions and foresee little difficulty in the management of this case as a class action.

80. Named Plaintiff is adequate and has no interest antagonistic to the Class and will fairly represent the interests of the Class in accordance with their affirmative obligations and fiduciary duties.

COUNT ONE
VIOLATION OF THE MARYLAND SAFE ACT
Md. Code, Est. & Trusts § 13-601, *et seq.*
On Behalf of the Class
(Against all Defendants)

81. Plaintiff re-alleges and incorporates by reference the allegations set forth above, and further alleges:

82. The Maryland Stop Adult Financial Exploitation (SAFE) Act, Md. Code, Est. & Trusts § 13-601, *et seq.*, constitutes remedial legislation that must be “construed and applied liberally to promote its purpose of deterring and remedying the financial exploitation of susceptible adults and older adults.” Md. Code, Est. & Trusts § 13-608.

83. As “persons” under the SAFE Act, Defendants are prohibited from committing financial exploitation against susceptible adults and older adults.

84. At all times relevant to this Complaint, Plaintiff was an “older adult” because she has been “at least 68 years old.” Md. Code, Est. & Trusts § 13-601(i).

85. The SAFE Act prohibits Defendants from financially exploiting older and susceptible adults in two ways relevant to the instant case.

86. First, financial exploitation means an act taken by a person who “[s]tands in a position of trust and confidence with a susceptible adult or older adult and who knowingly obtains or uses, or endeavors to obtain or use, a susceptible adult’s or older adult’s funds, assets, or property with the intent to temporarily or permanently deprive the susceptible adult or older adult of the use, benefit, or possession of the funds, assets, or property for the benefit of someone other than the susceptible adult or older adult, in such a manner that is not fair and reasonable.” Md. Code, Est. & Trusts § 13-601(e)(i).

87. “Position of trust and confidence” means “a relationship, whether formed by a formal or informal agreement between a susceptible adult or older adult and another person or recognized by a formal declaration or court order, in which: (1) A person is entrusted with the use or management of the property or assets of the susceptible adult or older adult, or the susceptible adult’s or older adult’s care; or (2) There is a special confidence or trust placed in a person who, in equity and good conscience, is bound to act in good faith and with due regard to the interests of the susceptible adult or older adult.” Md. Code, Est. & Trusts § 13-601(j).

88. Defendants stood in a position of trust and confidence with Plaintiff and Class Members because their relationship was formed by a formal agreement because ATM users consent to Athena’s Terms of Service. Furthermore, they are entrusted with the use of older adult’s assets because older adults insert their cash into the machines with the belief that the money will be protected by the owners of the machines.

89. Defendants knowingly obtained money from Plaintiff and Class Members with the intent to either temporarily or permanently deprive them of the funds. Defendants know that when

customers convert cash to cryptocurrency and send it to another person's wallet, they are permanently deprived of the funds.

90. Furthermore, Defendants possess the requisite intent because they could easily take more effective steps to deter, stop, and mitigate fraud yet choose not to do so. They know their action will cause that people like Plaintiff to be harmed for "the benefit of someone other than the susceptible adult or older adult."

91. Defendants' scheme is neither fair nor reasonable because their inaction is calculated to boost their profits at the expense of some of the most vulnerable residents of Maryland.

92. Second, financial exploitation means an act taken by a person who "[b]y deception, false pretenses, false promises, larceny, embezzlement, misapplication, conversion, intimidation, coercion, isolation, excessive persuasion, or similar actions and tactics, obtains or uses, or endeavors to obtain or use, a susceptible adult's or older adult's funds, assets, or property with the intent to temporarily or permanently deprive the susceptible adult or older adult of the use, benefit, or possession of the funds, assets, or property for the benefit of someone other than the susceptible adult or older adult." Md. Code, Est. & Trusts § 13-601(e)(ii).

93. Defendants used deception, false pretenses, false promises, and similar actions and tactics to obtain older adult's funds with the intent to permanently deprive them of the funds for the benefit of fraudsters.

94. Defendants advertise their machines as secure yet take no meaningful steps to make that a reality. Defendants intentionally shroud their machines in a veil of security, creating a false pretense that the transaction is akin to others that older adults would be familiar with, like cashing a check at a grocery store, depositing cash with a banker teller, or using a legitimate ATM.

95. Defendants' machines request driver's licenses and/or Social Security numbers from customers. These requests create an illusion of security yet do nothing to stop the most common types of scams. These illusions play into the narratives of the fraudsters, who direct their unsuspecting victims to Athena ATMs with promises that the machines are "encrypted" and therefore safe from the fictional threat they have invented.

96. Despite these empty gestures toward security, Defendants knowingly refuse to enact any measures that would effectively intervene, mitigate, or deter the use of its ATMs in scams such as the one in this case.

97. Defendants' actions, representations, misrepresentations, violations, and intimidation have caused damages to Plaintiff and Class Members.

98. Claims under the Maryland SAFE Act survive the death of the older adult. Md. Code, Est. & Trusts § 13-605(b)(2).

99. The statute of limitations under the Maryland SAFE Act is five years from the discovery of financial exploitation. Md. Code, Est. & Trusts § 13-607(a).

100. The Maryland SAFE Act allows susceptible and older adults to recover compensatory damages, restitution, declaratory relief, injunctive relief, reasonable attorney's fees, and treble damages, all of which Plaintiff and Class Members seek and are entitled to. Md. Code, Est. & Trusts § 13-606(c).

COUNT TWO
NEGLIGENCE
(Against all Defendants)

101. Plaintiff re-alleges and incorporates by reference the allegations set forth above, and further alleges:

102. Defendants are expressly aware of the risk of financial abuse and has made affirmations to the public and its customers that it "ensures safe and secure banking." Accordingly,

Defendants have assumed a duty to Plaintiff and Class Members to take reasonable steps to prevent the financial exploitation of older adults taking place at Athena ATMs.

103. As a financial services company, Defendants also owed a statutory duty to be aware of Plaintiff's and Class Members' status, age, and risk of being victimized under its "Know Your Customer" Rule under the PATRIOT Act and, if it did so, would have recognized that Plaintiff and Class Members were victims.

104. Plaintiff and Class Members, as senior citizens, are well-recognized within the cryptocurrency industry as a target for elder financial abuse, even according to Athena's own website that displays a telephone number for the AARP's fraud watch helpline.

105. The transaction at issue in this case was atypical and replete with red flags suggesting a scam. Those red flags should have triggered an alert to Defendants because they involved a seventy-five-year-old woman depositing \$13,000 at an Athena ATM for the first time, into a Bitcoin wallet that belonged to someone else.

106. Defendants breached their duties to Plaintiff and the Class by negligently, recklessly, and knowingly failing to implement checks and procedures both at Athena ATMs and internally that would effectively intervene, mitigate, or deter the use of Athena ATMs in scams such as the one in this case.

107. Through their actions and inactions, Defendants participated in and materially aided in the financial exploitation of Plaintiff and the Class. Without Defendants' actions and failures, this exploitation would not have occurred.

108. Defendants' negligent, reckless, and knowing failure and refusal to implement appropriate and sufficient checks and procedures to intervene, mitigate, or deter the use of the Athena ATMs described above in the subject scam was a direct and proximate cause of Plaintiff

and Class Members being scammed out of their money, while Defendants gained a profit as a direct result of the scam.

COUNT THREE
PRODUCTS LIABILITY: DESIGN DEFECT
(Against all Defendants)

109. Plaintiff re-alleges and incorporates by reference the allegations set forth above, and further alleges:

110. Defendants are manufacturers of a defective product and are liable for both negligence and strict liability claims of design defect.

111. Defendants are expressly aware of the risk of financial abuse and have made affirmations to the public and its customers that it “ensures safe and secure banking.” Accordingly, Defendants have assumed a duty to take reasonable steps to prevent the financial exploitation of older adults at its Athena ATMs.

112. Defendants breached these duties to Plaintiff and Class Members by negligently, recklessly, and knowingly failing to implement checks and procedures both at its ATMs and internally that would effectively intervene, mitigate, or deter the use of its ATMs in scams such as the one in this case.

113. Specifically, Defendants were negligent in designing and manufacturing Athena ATMs 1) in a manner that facilitates financial exploitation of users; 2) without appropriate warnings or instructions that would prevent the financial exploitation of users; and 3) without appropriate fail safes to monitor use of the machine to prevent financial exploitation of users.

114. Defendants are capable of implementing effective and sufficient checks and procedures both at the Athena ATMs and internally that would intervene, prevent, mitigate, or deter the use of the Athena ATMs in scams such as the one in this case, but knowingly choose not

to adopt effective checks or balances because doing so would thwart a substantial volume of their business and the profits they gain from every dollar inserted into the ATM.

115. The Bitcoin ATMs and their software programs are defectively designed because they allow criminals to easily use them to perpetrate financial scams. This defect is attributable to Defendants because they manufacture and operate the machines. The defect is causally related to the injuries suffered by Plaintiff and Class Members because criminals exploited the machines' design defects to steal money from Plaintiff and Class Members. The harm suffered by Plaintiff and Class members was reasonably foreseeable because Athena ATMs have become a known way for criminals to perpetrate fraud.

116. Turning to the elements of a design defect in strict liability, the Athena ATMs were in a defective condition at the time they left the possession or control of Defendants. The ATMs were unreasonably dangerous to consumers and the defect caused Plaintiff and Class Members' injuries. Finally, the product was expected to and did reach Plaintiff and Class Members without substantial change in its condition. Thus, Defendants are strictly liable for the design defect.

117. As a direct and proximate result of Defendants' placing a defective and unreasonably dangerous product into the stream of commerce, Plaintiff and Class Members have suffered damages to their property in the form of loss of title to cash assets deposited into the machines.

COUNT FOUR
VIOLATION OF THE MARYLAND CONSUMER PROTECTION ACT
Md. Code, Com. Law § 13-101, *et. seq.*
(Against all Defendants)

118. Plaintiff re-alleges and incorporates by reference the allegations set forth above, and further alleges:

119. Maryland's Consumer Protection Act ("CPA"), Md. Code, Com. Law § 13-101, et seq., constitutes remedial legislation that is intended to be construed liberally in order to promote its purpose of providing a modicum of protection for the State's consumers. *Wash. Home Remodelers, Inc. v. State, Office of Attorney Gen., Consumer Prot. Div.*, 426 Md. 613, 630 (2012).

120. As "persons" under the CPA, Md. Code, Com. Law § 13-101(h), Defendants are prohibited from engaging in unfair and deceptive trade practices.

121. At all times relevant to this Complaint, Plaintiff and Class Members were consumers because they purchased and received consumer services, namely converting their personal assets into cryptocurrency.

122. The CPA specifically prohibits Defendants from making false statements which have the capacity of deceiving or misleading consumers and failing to state a material fact if the failure deceives or tends to deceive. Md. Code, Com. Law §§ 13-301(1) and (3).

123. Defendants knew or should have known that their Athena ATMs were not secure and could easily be used for financial exploitation.

124. Defendants did not inform Plaintiff and Class Members about material facts concerning the common ways that criminals use their Athena ATMs to perpetrate financial exploitation, except perhaps buried in a nonexplicit Terms of Service agreement they knew few, if any, victims would actually read.

125. Defendants did not inform Plaintiff and Class Members about material facts concerning their failure to implement checks and procedures both at its ATMs and internally that would effectively intervene, mitigate, or deter the use of its ATMs in scams such as the one in this case.

126. Defendants intended that Plaintiff and Class Members rely on Defendants' misrepresentations and concealment, suppression, or omission of the material facts regarding the use of their ATMs for financial exploitation and regarding their own inaction.

127. Plaintiff and Class Members would not have used the Athena ATMs had they known the machines were routinely used for financial exploitation and that Defendants had knowingly failed to implement checks and procedures both at its ATMs and internally that would effectively intervene, mitigate, or deter the use of its ATMs in scams such as the one in this case.

128. Because the material facts were withheld, Plaintiff and Class Members were deceived and were damaged as a result.

129. In violation of the CPA, Md. Code, Com. Law §§ 13-301(1), (2), and (3) and 13-303(1) and (2), Defendants failed to state material facts and knowingly concealed, suppressed, or omitted material information regarding the security of the Athena ATMs with the intent that Plaintiff and Class Members rely on same.

130. Named Plaintiffs and Class Members seek to recover damages and their attorneys' fees from Defendants.

COUNT FIVE
DECLARATORY AND INJUNCTIVE RELIEF
On Behalf of the Class
(Against all Defendants)

131. Plaintiff re-alleges and incorporates by reference the allegations set forth above, and further alleges:

132. Named Plaintiff seeks a declaration individually and on behalf of the Class that Defendants are not entitled to manufacture and operate Athena ATMs without taking reasonable steps to effectively intervene, mitigate, or deter the use of its ATMs in scams.

133. Defendants should be ordered to disgorge all fees they collected from Class Members.

134. Defendants should be enjoined from manufacturing and operating Athena ATMs without taking reasonable steps to effectively intervene, mitigate, or deter the use of its ATMs in scams.

135. Defendants should be enjoined from profiting off their own inaction.

WHEREFORE, as to the claims set forth above, Plaintiff prays that the following relief be granted to the Named Plaintiff and the Class:

- A. The Court certify a class of persons as set forth herein or as may be amended, and appoint the Plaintiff as Class Representative and their counsel as Class Counsel;
- B. The Court order that Defendants pay to Named Plaintiff and members of the Class all compensatory and treble damages, including by refunding all predatory fees Defendants charged;
- C. The Court enter an award of pre-judgement and post-judgment interest on all sums awarded to Named Plaintiff and members of the Class;
- D. The Court award to Named Plaintiff and members of the Class reasonable counsel fees and the costs of these proceedings; and
- E. The Court order such other and further relief as the nature of this case may require.
- F. In order to comply with the Maryland Rules, the amount sought for damages is in excess of \$75,000.

Respectfully submitted,

/s/ Vaughn Stewart

Vaughn Stewart, CFPF No.: 2305040018
Matthew Thomas Vocci, CFPF No.: 0612130424
Santoni, Vocci & Ortega, LLC
201 W. Padonia Road, Suite 101A
Lutherville-Timonium, Maryland 21093
Phone: 443-921-8161

Fax: 410-525-5704
vstewart@svolaw.com
Attorneys for Named Plaintiff and Putative Class

/s/ J. Patrick McNichol
J. Patrick McNichol, CFPF No.: 1312180233
Kelly Guzzo, PLC
395 Chain Bridge Road, Suite 202
Fairfax, VA 22030
Phone: 703-424-7572
Fax: 703-591-0167
pat@kellyguzzo.com
Attorney for Named Plaintiff and Putative Class

CLAIM FOR ATTORNEY'S FEES

Named Plaintiff reiterates that, as stated in the individual counts for relief, she intends to seek attorneys' fees pursuant to Maryland Rule 2-701, *et seq.*, and these fees may be substantial as litigation continues.

/s/ Vaughn Stewart
Vaughn Stewart, CFPF No.: 2305040018

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the Class Members, demands trial by jury.

/s/ Vaughn Stewart
Vaughn Stewart, CFPF No.: 2305040018